AMENDMENTS TO THE SPECIFICATION

1. Please insert the following paragraphs into the Specification between the paragraph ending on pg. 2, ln. 24 and the paragraph beginning on pg. 2, ln. 25. Support for the following paragraphs comes from United States Provisional Patent Application Serial Number 60/111,497, Attachment H, previously incorporated by reference. No new matter is submitted.

In addition, user digital communications addresses such as internet or IP addresses are conventionally associated with a fixed physical location, such as a user's business telephone line. However, portable communications devices such as laptop computers are becoming increasingly popular, and it is common for a user to access the internet from locations as diverse as hotel rooms and airplanes.

Digital communications networks are set up to route communications addressed to a communication address to the associated physical location. Thus, if a laptop computer is connected to a remote location, communications to and from the computer will not be associated with the user's communications address.

In order for a computer (host) to communicate across a network (e.g., the internet), software protocols (e.g., Transport Control Protocol/Internet Protocol (TCP/IP)) must be loaded into the host. A host computer sends information (i.e., packets of data) to devices on the network (routers) which receive the packets and send the packets back to the destination host.

The destination host will route replies back using a similar process. Each host computer and router must be configured so it will know who to send the packets of data to. A router will receive the packets only if the host computers specifically send (address) the packets to that router. If a host is configured incorrectly (bad address), then the host computer and router will be unable to communicate.

With the advent of mobile computers (laptops) and the desire to plug them into various networks to gain access to the resources on the network and internet, a mobile computer must be configured for each network it plugs into.

Traditionally this new configuration can be done either (i) manually in software on the mobile computer (usually causing the mobile computer to be restarted to load in the new configuration), or (ii) with a new set of protocols which must be utilized on the mobile computer to obtain the configuration information from a device on the network to which the computer is being connected. When new services (protocols) are created to add functionality to the host computers, these new protocols must be updated in the host computers or routers, depending upon the type of new functionality being added.

2. Please insert the following paragraphs into the Specification after the paragraph ending on pg. 7, ln. 30. Support for the following paragraphs comes from United States Provisional Patent Application Serial Number 60/111,497, Attachment H, previously incorporated by reference. No new matter is submitted.

According to another embodiment, a portable "Nomadic" router or translator is provided. The nomadic router enables a laptop computer or other portable terminal which is configured to be connected to a local home network to be connected to any location on the internet or other digital data communication system. The nomadic router automatically and transparently re-configures the terminal to its new location and processes outgoing and incoming data:

The nomadic router includes a processor which appears as the home network to the terminal, and appears as the terminal to the communication system. The terminal has a permanent address, the nomadic router has a router address, and the terminal transmits outgoing data to the system including the permanent address as a source address. The processor translates the outgoing data by replacing the permanent address with the router address as the source address. The terminal receives incoming data from the system including the router address as a destination address, and the processor translates the incoming data by replacing the router address with the permanent address as the destination address.

The terminal can be directly connected to a point on a local network, and the nomadic router connected to another point in the network. The nomadic router can be employed to implement numerous applications including nomadic e-mail, network file synchronizer, database synchronizer, instant network, nomadic internet, mobile virtual private network and trade show router, and can also be utilized as a fixed nomadic router.

The nomadic router can be implemented as software and/or hardware. The nomadic router establishes location and device transparency for a digital communication terminal such as a laptop computer. The terminal can be connected to any of a variety of networks and locations which can employ a variety of communication interface devices.

The nomadic router automatically converts the actual location address to a unique communication address for the user such as an internet address, such that the terminal performs communications originating from the communication address regardless of the physical location of the terminal.

The nomadic router also automatically configures the terminal to utilize a selected one of the interface devices, and switches from one to another if the first device malfunctions or becomes otherwise unavailable.

The nomadic router includes software and services which can be packaged in a personal portable device to support a rich set of computing and communications capabilities and services to accommodate the mobility of nomads (users) in a transparent, integrated, and convenient form. This is accomplished by providing device transparency and location transparency to the user.

There is a vast array of communication device alternatives such as Ethernet, Wireless LAN, and dialup modem among which the users switches when in the office, moving around the office, or on the road (such as at a hotel, airport, or home). The device transparency in the nomadic router provides seamless switching among these devices (easily, transparently, intelligently, and without session loss. The location transparency support in the nomadic router

prevents users from having to reconfigure (e.g., IP and gateway address) their network device (laptop) each time they move to a new network or subnetwork.

The present nomadic router provides a separation of location and identity by providing a permanent IP address to the network device (host). The nomadic router provides independence between the location, communication device, and the host operating system. There are no new standards need to be adopted by the networking community. All specialized processing is stored internally to the nomadic router with standard interfaces to the host device and various communication devices.

The nomadic router supports the migration to Network Computers by providing identity and security services for the user. The nomadic router also supports multiple parallel communication paths across the communications network for soft handoff, increased throughput, and fault tolerance by supporting multiple communication substrates.

A portable router for enabling a data communication terminal to be location and device transparent according to the present invention, comprises: a first module for storing a digital communication address of a user; a second module for detecting a data communication network location to which the terminal is connected; a third module for detecting communication devices that are connected to the terminal; a fourth module for establishing data communication between the terminal and the network such that the communication address of the location from the second module is automatically converted to the communication address of the user from the first module; and a fifth module for automatically selecting a communication device which was detected by the third module for use by the fourth module.

The present nomadic router utilizes a unique process embodied in a self-contained apparatus which manipulates the packets of data being sent between the host computers and routers. This process provides an intelligent active universal translation of the content of the packets being transmitted between the host

computer and nomadic router. The translation allows the host computer to communicate with the nomadic router even when the host computer is not configured to communicate with the nomadic router.

This is achieved by the nomadic router pretending to be the router which the host is configured for, and by the nomadic router pretending to be the host which the router expects to communicate with. Therefore, the nomadic router supports the mobility of computers in that it enables these computers to plug into the network at different locations *(location independence)* without having to install, configure, or utilize any new protocols on the mobile computer.

The mobile computer continues to operate without being aware of the change in location or new configuration, and the nomadic router translates the data allowing the host to think that it is communicating with the router. By putting this process in a self-contained apparatus, the deployment of new protocols can be performed independently of the host computer and its operating system *(host independent)*.

All specialized processing and translation is stored internally in the nomadic router with standard interfaces to the host device and various communication devices. Thus, no new standards need be adopted. By removing the complexity of supporting different network environments out of the mobile computer and into this self-contained apparatus, the nomadic router allows the host computer to maintain a very minimal set of software protocols and functionality (e. g., the minimum functionality typically installed in network computers) to communicate-across the network.

The nomadic router translation ability also enables the use of alternate communication paths *(device independence)* without the host computer being aware of any new communication device that utilizes an alternate communication path. The translation of the packets is done not just at the physical, link, or network layer of the protocol stack but at the transport and application layers as

well. This allows the network card, protocol stack, and application running on the host computer to be independent of the network environment and configuration.

As an example of the communication device independence, the translation allows soft handoff, increased throughput, and fault tolerance by supporting multiple communication substrates. In addition, the nomadic router translation ability provides a flexible process for deploying enhanced nomadic and mobile computing software and services such as filtering of packets and determining which packets should be allowed to be transmitted between the mobile computer and the nomadic router or local area network (Internal Firewall).

The router apparatus can be: (i) carried with the mobile user (e.g., using an external box); (ii) attached to the mobile computer (e.g., PCMCIA card); (iii) installed inside the mobile computer (e.g., a chip in the laptop); (iv) or installed into the network infrastructure so it will already be there when the mobile computer user arrives (e. g ., a box which plugs into the local area network translating packets being sent between the host and nomadic router, or a chip which is installed in routers on the network). The nomadic router can also be provided in the form of software which is loaded into and run in the mobile computer or another computer or router on a network.

These and other features and advantages of the present invention will be apparent to those skilled in the art from the following detailed description, taken together with the accompanying drawings, in which like reference numerals refer to like parts.

3. Please insert the following paragraphs into the Specification after the paragraph ending on pg. 8, ln. 5. Support for the following paragraphs comes from United States Provisional Patent Application Serial Number 60/111,497, Attachment H, previously incorporated by reference. No new matter is submitted.

FIG. 2 is a diagram illustrating the implementation of the present nomadic router between the host computing device and various communication devices through standard interfaces;

FIG. 3 is a diagram illustrating the basic nomadic router architecture, which is referred to as the hardware implementation architecture;

FIG. 4 is a flowchart illustrating a configuration overview of the basic steps performed when a host device is attached to the present nomadic router and when a network interface is attached to the router;

FIG. 5 is a flowchart illustrating the router's automatic adaptation to the host device when the first data packet from the host is sent to the attached router or when an activation interrupt or signal is received;

FIG. 6 is a flowchart illustrating the process by which the router initializes and checks the various communication device interfaces for initialization, activation, etc.;

FIG. 7 is a diagram illustrating the basic nomadic router architecture when implemented as software in the host device;

FIGS. 8a to 8g are diagrams illustrating protocol stack implementations for various network devices, and the translation function happening at all layers of the protocol stack in the nomadic router;

FIG. 9 is a flowchart illustrating the nomadic router's proxy ARP packet interception and host reconfiguration process;

FIGS. 10a and 10b in combination constitute a flowchart illustrating the nomadic router's translation process which takes place in the host computer and nomadic router at various levels in the protocol stack;

FIGS. 11a to 11d are diagrams illustrating host and network interface modes in which the nomadic router is able to operate;

FIG. 12 is a simplified perspective view illustrating the nomadic router as implemented in a self-contained box which connects onto a local area network via a network interface port and has multiple ports to connect to host computers;

FIG. 13 is a simplified perspective view illustrating the nomadic router apparatus as implemented on a PCMCIA Type III card where the nomadic router plugs into the host computer's type II slot and the communication card device, of Type II, plugs directly into the nomadic router so both may be powered and stored in the portable host computer; and

FIG. 14 is a simplified perspective view illustrating the nomadic router as implemented on a PCMCIA Type II card where the nomadic router plugs into the host computer via a type II interface slot and where the communication card device, Type II, plugs into the nomadic router type II card.

4. Please insert the following paragraphs into the Specification after the paragraph ending on pg. 9, ln. 29. Support for the following paragraphs comes from United States Provisional Patent Application Serial Number 60/111,497, Attachment H, previously incorporated by reference. No new matter is submitted.

FIG. 2 illustrates a "Nomadic" translator or router 110 embodying the present invention as being connected between a host device or computer 112 and a communications device 114. The host device 112 is a laptop computer or other fixed or mobile digital data communication terminal which is sufficiently portable or mobile that it can be carried from one location or another. A laptop computer, for example, can be used in any convenient location such as an airplane, customer's office, home, etc.

The communications device 114 can be part of any type of communication system to which the host computer 112 can be connected. Such communication systems include, but are not limited to, local networks, wide area networks, dial-

up and direct internet connections, etc. In a typical application the communications device will connect the host computer to a local network which itself is connected to the internet. Thus, the host device 112 is able to communicate with an unlimited number of networks and nodes which are themselves interconnected with routers, switches, bridges, etc. in any known manner.

The present router 110 includes a terminal interface 110a which normally is used to connect the router 110 to the host device 112, and a system interface 110b which connects the router 110 to the communications device 114. As will be further described below, the router 110 generally includes a processor consisting of hardware and/or software which implements the required functionality. The router 110 is further configured to operate in an alternate mode in which the host device 112 is connected directly to a network, and the router 110 is also connected to a point in the network via the system interface 110b. In this case, the terminal interface 110as is unused.

Although the device 110 is described herein as being a router, it will be understood that the router 110 is not a conventional router in that it includes the capability for providing interconnectability between networks. Instead, the present router 110 is essentially a translator which enables the host device 112 to be automatically and transparently connected to any communications device 114, and process incoming and outgoing data for the device 122.

The host device 112 is provided with a permanent internet address which is conveniently not changed in accordance with the present invention. The device 122 is also initially configured to communicate with a particular gateway or other home device at its base location. The gateway has a home address which the device 122 attempts to locate when it is connected to any communication system. Without the functionality of the present nomadic router 110, the host device 122 would not be able to operate at a remote location because it would not find its gateway.

It will be understood that the term "home" does not relate to a residence, but is the network, gateway or other communication device or system to which the terminal is normally connected and which corresponds to the home internet or IP address.

FIG. 2 further illustrates a top protocol layer 116 representing the host computing device 112 which generates and consumes data that is transferred through the communications device 114. This interface 116 is done just below the IP layer, and above the link layer in the typical OSI/ISO model. In the middle is a layer 118 which represents the router 110 and whose function it is to adaptively configure and utilize the underlying communications device and provide the router support described herein. A lower layer 120 is a physical communication which carries out the communication (potentially wire-lined Internet based, ad-hoc or wireless) as made available and determined for use by the nomadic router or user. Between the router layer 118 and the layers 116 and 120 are interfaces 122 and 124 which the router 110 identifies and configures dynamically.

The present router operates with host computers, routers, and other network devices through well-defined standard interfaces such as specified by the IETF (Internet Engineering Task Force) and IEEE standardization committees. These standards specify the packet format, content, and physical communication characteristics. As shown in FIG. 8a, host computers have to be configured at various layers of the protocol stack depending on the communication capabilities and configuration of the current network being attached to.

Hubs, as shown in FIG. 8b, provide a well-defined interface to connect host computers and network devices by transmitting packets across multiple physical connections. Hubs do not provide any manipulate or translation of the content of the packets being transmitted.

Bridges or switches, as shown in FIG. 8c, provide an intelligent filtering mechanism by which they only transmit packets across multiple physical

connection based upon which physical connection the device is connected to, according to the link layer addressing (Media Access Control Address). Bridges and switches do not manipulate the content of the packet and do not provide any higher layer protocol functionality.

Routers, as shown in FIG. 8d, accept packets based upon the destination address at the network layer in the packet. The host computer must explicitly address the packet at the link layer to the router. The router will then retransmit the packet across the correct physical connection based upon how it is configured. No modification or translation of the packet is performed at any layer of the protocol stack other than the network layer.

Firewalls, as shown in FIG. 8e, filter packets at the network and transport layers to only allow certain packets to be retransmitted on to the other physical connection. Firewalls do not manipulate the content of the packet, only forward it on to the next hop in the network if it passes the transport (port) or network (IP address) filter.

Proxys and gateways, as show in FIG. 8f, only receive packets explicitly addressed to them by host computers. They only manipulate packets at the application level. The present nomadic outer 110, as shown in FIG. 8g, manipulates the content of the jackets at the link, network, transport, and application layers of the protocol stack to provide a translation between how the host computer is configured and the configuration of the network the host computer is currently attached to.

Unlike all other devices shown in FIGS. 7a to 7f, the router 110 will automatically intercept and translate packets without the other devices being aware of the router 110 or have to be configured to use it. The translation algorithms in the router 110 which provide this location independence are provided completely internal to the router 110. Thus no new standards need to be developed, accepted, or implemented in host computers 112 or routers 126 to deploy new network services when using the nomadic router.

Whenever a new or different communication device (which includes the link and physical layers) is utilized in a host computer 112, the host computer's network layer must be aware of this new communication device. Since the router 110 has it's own network interface to the communication device, alternate communication devices can be utilized in the router 110 which the host computer 112 can utilize but does not have to be configured to use.

Permanent Addressing not Location Based

Today we communicate with individuals in terms of the location of their communications instruments (for instance, their computer's IP address or their fax machine's phone number). In order to support mobility and changing communication environments and devices, it is necessary to create an environment where people communicate with other people, and not specifically with the devices they use. To transparently support mobility and adaptivity in a wireless, potentially ad-hoc, communication internetwork, a common virtual network must be provided by an intelligent device or agent which supports the various computing hosts and communication devices.

The present nomadic router 110 provides the mapping between the location based IP address used in the Internet today and the permanent user based address housed in the host CPU in the device 112. This is illustrated in FIG. 3 as "IP Mapping". This mapping is done without support or knowledge of such mapping by the host CPU or user.

The Internet RFC 2002 Mobile IP protocol specifies the mapping between permanent and temporary IP addresses. The unique aspect of the nomadic router is that the Mobile IP protocols are not necessarily running in, or supported by, the host CPU but rather are internal to the nomadic router. The host configuration information such as its IP number are discovered or determined as illustrated -- in FIG. 5 and stored in the nomadic router 110 as illustrated in FIG. 3 as "Host Info." This configuration process is overviewed in FIG. 4.

Optional Off-loaded Processing

As illustrated in FIG. 3, the nomadic router 110 can provide off-load communication processing for the host CPU by being physically separate from the host device 112. The adaptation, selection, and transportation of information across the network is performed by the nomadic router 110. This allows the host terminal or device 112 to utilize the network without having to directly support the network protocols. By having the nomadic router be responsible for adapting to the current network substrate, the host CPU can maintain a higher performance by not having to run the routing, adaptation, packetization, etc. algorithms or packet processing.

The nomadic router can also queue, transmit, and receive data independent of whether or not the host device 112 is available or even attached. The CPU 11 built into the nomadic router 110 provides all necessary computing routines to be a fully functional network co-processor independent of the host CPU. This will allow increased battery for the user since the nomadic router does not have numerous user I/O devices as does the host device 112.

Location Independence

The instant network nomadic router provides the ability to provide ubiquitous and reliable support in a location independent fashion. This removes any burden on the user for device reconfiguration (e.g., IP address configuration, gateway or next hop router address, netmask, link level parameters, and security permissions) or data transmission.

The problem with existing protocol stacks is that communicating devices have to be reconfigured every time the communication environment changes. TCP/IP requires a new network, node and gateway number. Appletalk will automatically choose an unused node number and discover the network number, but all open communications are lost and services have to be restarted to begin using the new information.

This occurs, for example, when a PowerBook is plugged into a network, put to sleep, and then powered up in a different network. All network services,

are restarted upon wakeup, and network applications get confused if they, are not restarted. The nomadic router solves this problem by providing temporary as well as permanent network and node numbers similar, to that provided by Mobile IP. However, the nomadic router will also work with other protocol stacks (e.g., AppleTalk).

Mobile IP provides location independence at the network level and not at the link level. All link level parameters, which are device specific, will be automatically configured as illustrated in FIG. 6 when a new communications (network interface) device is attached to the nomadic router. The nomadic router completely eliminates the need for manual configuration by adaptively supporting device independence.

A problem with existing routers today is that they require manual configuration and exist external to the node. To overcome this, the nomadic router can support automatic configuration and full router functionality internally. This allows a mobile or nomadic node to adapt to various communication and network devices dynamically, such as when the user plugs in a PCMCIA card or attaches a communications device to the serial port.

Once the nomadic router becomes aware of the available communication devices and activates them, the transport of data across the multiple communication substrates can take place. The unique algorithm and protocol in the nomadic router which chooses the most appropriate device to use, is shown in FIG. 3 and FIG. 6 as part of the nomadic router Device Checker through the "nomadic router Device Selection" across each interface.

There are numerous factors that can affect the selection of utilizing one or more devices. Such factors typically include available bandwidth, cost to initiate and maintain connection, power requirements and availability, and user's preference.

Another feature of the nomadic router is the support for alternate or simultaneous use of various communication substrates. This is performed as part

of step 5 in FIG. 7 when the source address is that of the communication substrate that the nomadic router is going to send the packet out on. Host computers will now indirectly be able to utilize two or more communication substrates, either to increase throughput or to provide soft-, handoff capability.

This functionality is not supported in today's typical protocol stacks (e.g., TCP/IP or AppleTalk). Once the nomadic router becomes aware of the available communication devices and activates them, the transport of data across the multiple communication substrates can take place. The unique algorithm and protocol in the nomadic router which chooses the most appropriate device to use is part of the "nomadic router Device Checker" through the "nomadic router Device Selection" across each interface.

There are numerous factors that can affect the selection of utilizing one or more devices. Such factors typically include available bandwidth, cost to initiate and maintain connection, power requirements and availability, and user's preference.

Apparatus Packaging

As described above, the nomadic router can be packaged in several different hardware configurations. The nomadic router can be embedded in the host computer, or network device such as a switch or router. It can also be implemented as a PCMCIA card which plugs into the host computer or as self-contained external box.

Each nomadic router can have from one to many interfaces. If the router 110 is put into the network infrastructure, it doesn't have to be carried around with the mobile user. As shown in FIG. 11a, the nomadic router 110 is attached to a Local Area Network (LAN) of the network infrastructure which constitutes the communications device 114 through the system interface 110b. The LAN 114 is connected through a conventional router 126 to the internet 128. In this case, the host computer interface 110a of the nomadic router 110 is not needed since packets from the host computer 112 are received through the LAN 114.

To provide a secure interface between the host computer 112 and network 114 to prevent host computers from being able to watch (sniff) packets on the network 114, the nomadic router 110 can have one interface to the host computer 112 (terminal interface 110a) and a second interface (110b) to the network 114 as shown in FIG. 11b, and provide filtering to which packets and retransmitted between the various interfaces thus providing a firewall type of security device but which operates internally on the network.

In order to support multiple host computers 112a ... , 112n with a single nomadic router 110, the nomadic router 110 may have multiple host interfaces $110a_1$, ... $110a_n$ as shown in FIG. 11c and in FIG. 12 and a network or system interface 110b.

If the nomadic router is carried around by the mobile user, it can take the form of a PCMCIA card. In FIG. 11d, the nomadic router 110 is implemented as a PCMCIA card. The processing and translation capability is stored inside the card and the interface to the host computer 112 is through a PCMCIA BUS interface or communication card 130.

As shown in FIG. 13, the PCMCIA card can fit in a type III slot where there is a connector on the nomadic router 110 which accepts the communication card 130 (a type II PCMCIA card.) In this mode, the nomadic router doesn't not have to have the communication device specific components inside the PCMCIA card.

The nomadic router 110 can also take the form of a type II PCMCIA card. In this form, the communication device or card 130 plugs into the opposite end of the nomadic router card 110 as illustrated in FIG. 14.

TRANSLATION OPERATION OF THE NOMADIC ROUTER

Initialization and Self Configuration

The nomadic router initialization and self configuration process provides the means by which the nomadic router is able to learn about the host computer and network so it knows what translation is necessary.

Host Learning

The nomadic router 110 is able to learn about how the host computer 112 is configured by looking at the content of the packets being sent from the host computer 112. Rather than the host computer 112 sending packets directly to the router 126 or other network device, which is what it is initially configured to do, the nomadic router 110 is able redirect all outbound packets from the host computer 112 to itself. This redirection can be accomplished in several ways as described below.

1. Proxy ARP Packet Interception and Host Reconfiguration

Whenever a host computer 112 has an IP packet which it needs to send to a router 126 or other network device, it uses the Address Resolution Protocol (ARP) to obtain the link layer Media Access Control address (MAC address). As illustrated in FIG. 9, when the host computer 112 broadcasts and ARP request for the MAC address of a destination node, the nomadic router 110 receives this ARP request broadcast and responds with its MAC address (not that of the destination node).

When the host computer 112 receives this ARP reply from the nomadic router 110, which contains the MAC address of the nomadic router 110, the host computer 112 will cache this MAC address in the host computer 112 and send all packets destined for the configured router or network device to the nomadic router 110. The host computer 112 will think that the MAC address is that of the configured IP network device, but in reality, the nomadic router 110 is pretending (proxying) to be the device (its home gateway) that the host computer 112 expects to find.

The nomadic router 110 is also able to reconfigure and intercept return packets from a router or other network device using the same process.

2. Promiscuous Mode Packet Interception

Since the MAC address is cached in the host computer 112 for a short period of time, the host computer 112 will not send out a new ARP request to

obtain the MAC address again unless a timeout period occurs or the cache is cleared such as when the computer 112 is restarted.

When a conventional network device receives or hears a packet with a MAC address which does not match its own, it will ignore or drop the packet. Since it is possible to rapidly switch from one network environment to another using a portable computer, the nomadic router 110 must be able to intercept packets even when the MAC address is not that of the nomadic router's home gateway or device.

This is accomplished by placing the nomadic router's network connection in promiscuous mode. In this mode, the network connection on the nomadic router accepts all packets being transmitted. on the communication link, not just ones being broadcasted or addressed specifically to it.

3. Dynamic Host Configuration Protocol (DHCP) Service

A host computer is able to utilize the DHCP service to obtain the configuration information rather than being manually configured. The host computer utilizing the DHCP service requires that a DHCP server be installed on the network segment to which it is currently attached. If the host computer 112 is utilizing this service and requests configuration information using DHCP, the nomadic router 110 will intercept these requests and respond with configuration information for the host computer 112 to use.

Network Learning

The nomadic router is able to learn about the network environment it is currently attached using several different methods as described below.

1. Dynamic Host Configuration Protocol (DHCP)

Whenever a different network connection is connected on the nomadic router, it will broadcast a DHCP request to obtain configuration information for the current network. If no DHCP service is available on the network, it will switch to another method to learn about the network configuration.

2. Router Information Packets

Routers on the network will periodically broadcast router information packets which are used to build routing tables and allow routers to adapt to changes in the network. The nomadic router 110 will listen on the network for these router information packets. When one is received, it will extract out the configuration information from these packets.

3. Passive Listening

By placing the nomadic router's network connection in promiscuous mode, where is receives all packets not just ones destined for it, it is able to examine all packets on the network to discover how the network is configured. It is also able to determine the IP addresses used on the local area network and which machines are routers by the final destination address not being the next hop address.

Using this method, the nomadic router 110 is passively able to learn how the network is configured and will elect to use an unused IP address. If that IP address does become used by another network device, it will switch over to another unused IP address.

4. Manual Configuration

The network configuration information can be manually configured in the nomadic router 110. This information' can be set using an embedded web server, Simple Network Management Protocol (SNMP) tools, an application running on one of the computers in the network, or other suitable means. When manual configuration is used to set the network information, the nomadic router 110 will still learn about the host information automatically and provide all the translation capabilities so the host computers do not have to be aware of the correct network information of the LAN to which they are currently connected.

Packet Translation

The nomadic router's packet translation function provides a mapping between location and service dependent configurations used by the host computer 112 and that used by the network 114 to which it is currently attached. For

outbound traffic from the host; computer 112 to the network 114, the translation function changes the content of the packet such as the source address, checksum, and application specific parameters, causing all packets sent out to the network 114 be directed back to the nomadic router 110 rather than to the host computer 112.

The inbound traffic from the network 114 arriving at the nomadic router 110, which is really for the host computer 112, is passed through the translation function so the host computer 112 thinks that the replies were sent directly to it. The host computer 112 will be completely unaware of all the translation being performed by the nomadic router 110.

The translation functions works as illustrated in FIGS. 10a and 10b. In these figures, the operations performed in the OSI/ISO model application, transport, network, link and physical layers are illustrated in rows opposite the layer designations. The operations performed by the host computer 112, nomadic router 110 and network 114 are illustrated in columns below the device designations.

The host computer 112 will generate network packets using the current configuration stored in the host computer 112 using the standard protocol stack as shown in step 1. This configuration information is either manually configured in the host computer 112 or obtained using DHCP.

As shown in step 2, when the host computer 112 addresses the link level destination address, the address automatically obtained using the Proxy ARP packet interception routine described earlier, this will cause the host computer 112 to send the packet to the network address of its standard router or home gateway device, but using the link level address of the nomadic router 110.

In step 3, the packet is transmitted across the standard physical connection between the host computer 112 and nomadic router 110. As shown in step 4, the nomadic router 110 will receive the packet at the link level either due to the Proxy ARP function which reconfigured the host computer's MAC address, or the

nomadic router 110 will have the link level in promiscuous mode which it will cause it to receive the packet even if destined to a different MAC address.

Once the packet is passed to the network layer, shown in step 5, the nomadic router translation function will modify the content of the packet to change the source address to that match of the nomadic router's address instead of the host computer's address. It will also translate other location dependent information such as the name of the local Domain Name Service (DNS) server. When translating the DNS packet, it will change the source address to that of the nomadic router's address and the destination address to that of a local DNS server.

Once the network layer translation is complete, the packet can be translated at the application and transport layers. The application layer is translated next, as shown in step 6, since the transport layer requires a pseudo network layer header which includes the source and destination addresses and the content from the application layer.

At the application layer translation, any addresses which describe the source address of the host computer, such as with FTP, are translated to be that of the nomadic router's address. Any application layer destination addresses, such as a local proxy server, are translated to match that of the server running on the current network.

Once this application translation is complete, the transport layer, as shown in step 7, can complete the checksum and any port number manipulation. The port number is manipulated if more than one host computer 112 is attached to the nomadic router 110. Each host computer 112 when it sends out a request using a specific port is translated to match an available inbound port on the nomadic router 110.

The port number assigned for use with each host computer 112 is stored in a table in the nomadic router 110 and is utilized with the reply packet described later. Finally the packet is sent out over the network 114 in step 8.

When a reply packet comes in from the network 114, as shown in step 9, the nomadic router 110 will receive the packet. In step 110, the nomadic router 110 will perform the reverse network layer translation to set the destination address to that of the host computer rather 112 than the nomadic router's address, and any source address to that replaced by the nomadic router 110 in step 5.

Once this network translation is complete, the packet is translated at the application layer, as shown in step 11, to change the destination address to that of the host computer 112 and the source address to the original destination address stored from step 6. In step 112, any port manipulation performed in step 7 is changed to the original setting and a new checksum is computed. Finally, as shown in step 13, the packet is sent to the host computer 112 which then processes the packet normally.

OPTIONS OF THE NOMADIC ROUTER

By way of motivation, many communication infrastructures are varied and fragmented, and this problem is likely to be exacerbated as more technologies are introduced. For example, high performance LANs, wireless services, cellular telephony, satellite, ubiquitous paging networks, all provide varying degrees of coverage, cost and bandwidth/delay characteristics.

Nomadic Intranet

The Nomadic Intranet provides all network, server type, services for users who which to dynamically create an ad hoc network. This is similar to the instant network nomadic router except the nomadic intranet is a single device with multiple ports into which laptop/devices can be plugged. The instant network nomadic router is distributed to (one per) each host device. The nomadic intranet not only provides ad hoc networking but can also provide services such as temporary file storage, protocol conversion, act as a print server, and provide other services described as part of the Basic nomadic router.

Fixed Nomadic Router

The Fixed nomadic router provides the same basic functionality and architecture as the portable nomadic router but is stored in one location. The fixed nomadic router acts as a surrogate or "Home Agent" for the user when he/she is away on travel. When the user wishes to register or utilize their host device elsewhere in the network, the portable nomadic router will register with the fixed nomadic router where it is temporarily attached to the network so information can be forwarded to the user's new location. The fixed nomadic router can also be used to house the master copy of the user's E-mail for the nomadic E-mail service, or files for the nomadic file synchronizer.

Mobile Virtual Private Network

The nomadic router provides the mapping between the location based IP address used in the internet today and the permanent user based address housed in the host CPU. This mapping is done without support or knowledge of such mapping by the host CPU or user. The Internet RFC 2002 Mobile IP protocol specifies the mapping between permanent and temporary IP addresses. The unique aspect of the nomadic router is that the Mobile IP protocols are not necessarily running in, or supported by, the host CPU but rather are internal to the nomadic router.

By implementing this protocol as part of the translation function in the nomadic router, the nomadic router can encapsulate packets from the host computer and transmit them back to the fixed nomadic router which are sent out (un-encapsulated) on the native (home) network. Replies from the home network are received by the fixed nomadic router and are encapsulated and sent back to the nomadic router. When packets are transmitted between the nomadic router and fixed nomadic router, the packets are encrypted and sent using the Internet Tunneling Protocol.

Since the nomadic router provides location independence and the fixed nomadic router forwards all packets from a corresponding host to the host computer via the nomadic router, any changes in the location, failure of a network

link, or attachment point of the mobile host computer does not cause any open session to be lost. This session loss prevention is possible since the fixed nomadic router pretends to be the mobile host computer, and the nomadic router pretends to be the home network. The fixed nomadic router and nomadic router translation functions hide the link and network loss from the transport and application session.

5. Please insert the following paragraph into the Specification between the paragraph ending on page 10, line 4 and the paragraph beginning on page 10, line 5. Support for the following paragraph comes from United States Patent No. 6,636,894, issued October 21, 2003, filed December 8, 1999, previously incorporated by reference. No new matter is submitted.

In order to allow a user of the computer to communicate transparently with computer networks 20 or online services 22, the gateway device must be able to communicate with the user computer, as well as the various online services 22 or networks 20. In order to support this communication, the gateway device 12 generally performs a packet translation function that is transparent to both the user and the network. In this regard, for outbound traffic from a computer to a network or on-line service, the gateway device 12 changes attributes within the packet coming from the user, such as the source address, checksum, and application specific parameters, to meet the criteria of the network to which the user has accessed. In addition, the outgoing packet includes an attribute that will direct all incoming packets from the accessed network to be routed through the gateway device. In contrast, the inbound traffic from the computer network or other online service that is routed through the gateway device undergoes a translation function at the gateway device so that the packets are properly formatted for the user's host computer. In this manner, the packet translation process that takes place at the gateway device 12 is transparent to the host, which appears to send and receive data directly from the accessed computer network. By implementing the gateway

device as an interface between the user and the computer network or other online service, however, the user will eliminate the need to re-configure their computer 12 upon accessing subsequent networks as well as the need to load special configuration software on their computer to support the reconfiguration.

6. Please amend the following paragraph beginning on pg. 16, ln. 29 of the Specification as follows:

Although the NAS 28 grants and denies access to users, the NAS 28 does not determine whether each user is allowed to connect to the network and, if so, what type of connection should be established. Rather, these determinations are made by the AAA server 30, ~~illustrated as exterior to the gateway device in FIG. 6, and~~ described in detail above. Upon receiving user data the NAS 28 can, if necessary, reconfigure the data such that the data will be in the proper format to be received by the AAA server 30. In addition to reconfiguring the user data, the NAS 28 can also encrypt the user data such that the user identity and password will be protected during transmission to the AAA server 30. After reconfiguration, and optionally, encryption, the NAS 28 transmits the data to the AAA server 30 with a query to request that the AAA server 30 authenticate the user

7. Please amend the following paragraph beginning on pg. 17, ln. 31 of the Specification as follows:

~~In the embodiment shown in FIG. 6,~~In an embodiment, the AAA server 30 is located outside of the gateway device, although it may alternatively be located within the gateway device. For example, the location of the AAA server 30 may be such that the NAS 28 communicates with the AAA server 30 via internet protocol. Therefore, it will be appreciated that the AAA server 30 may be located at any internet address and stored on any computer accessible via internet protocol. Locating the AAA server 30 outside the network can provide a number

of advantages. First, the administrative burden on the network is alleviated because the network does not have to set up and maintain separate authentication databases on each network or gateway device. This is especially important because each gateway device 12 allows a finite number of users to access the network, so that multiple gateway devices may be required. Secondly, administering and maintaining one consolidated database of authentication data is easier than multiple smaller databases.

8. Please append the following sentence before the paragraph beginning on pg. 19, ln. 23. Support for the following sentence comes from United States Patent No. 6,636,894, issued October 21, 2003, filed December 8, 1999, previously incorporated by reference. No new matter is submitted.

In an embodiment, the redirection is accomplished by a Home Page Redirect (HPR) performed by the gateway device, a AAA server, or by a portal page redirect unit located internal to or external to the gateway device.

9. Please insert the following paragraphs into the Specification between the paragraph ending on page 20, line 2 and the paragraph beginning on page 20, line 3. Support for the following paragraphs comes from United States Patent No. 6,636,894, issued October 21, 2003, filed December 8, 1999, previously incorporated by reference. No new matter is submitted.

According to one aspect of the present invention, when a user initially attempts to access a destination location, the gateway device, AAA server or portal page redirect unit receives this request and routes the traffic to a protocol stack on a temporary server, which can be local to the gateway device. This can occur where a user initially opens a web browser resident on the user's computer and attempts to access a destination address, such as an Internet site. The destination address can also include any address accessible via the network or an online service, and can include the portal page. The protocol stack can pretend to be the user-entered destination location long enough to complete a connection or `handshake`. Thereafter, this protocol stack directs the user to the portal server, which can be local to the gateway device to facilitate higher speed communication. The redirection to the portal server can be accomplished by redirecting web pages only, rather than all traffic, including E-mails, FTPs, or any other traffic. Therefore, once authorized, if a user does not attempt to access a webpage through the user's internet browser, the gateway device can forward the communication transparently to the user's requested destination without requiring

the user to access the portal page. Furthermore, according to one aspect of the invention specific user-input destination addresses may be authorized to pass through the gateway device without being redirected.

Furthermore, redirecting the user to a portal page can comprise redirecting the user to a portal page created by an administrator associated with the portal page, or redirecting the user to a portal page customized by the user.

The portal page can also be specialized based on the user, user's location, user's computer, or any combination thereof. For example, assuming that the user has been authenticated and has authorization, the gateway device can present users with a portal page that identifies, among other things, the online services or other computer networks that are accessible via the gateway device. In addition, the portal page presented by the gateway device can provide information regarding the current parameters or settings that will govern the access provided to the particular user. As such, the gateway administrator can readily alter the parameters or other settings in order to tailor the service according to their particular application. Typically, changes in the parameters or other settings that will potentially utilize additional resources of the computer system will come at a cost, such that the gateway administrator will charge the user a higher rate for their service. For example, a user may elect to increase the transfer rate at which signals are transmitted across the computer network and pay a correspondingly higher price for the expedited service.